The Business Case for IT Security as a Core Course in IS Curriculum

Emergent Research Forum (ERF)

Atiya Avery
University of Alabama in Huntsville
atiya.avery@uah.edu

Richelle L. Oakley
University of North Georgia
richelle.oakley@ung.edu

Abstract

As information systems within organizations have become more complex, interdependent, and dispersed, there is an increasing need for all employees to have an in-depth understanding of IT security. In this paper, we discuss the need for the information systems domain to better address the shortage of cybersecurity professionals by ensuring that IT security is considered as a core course in IS curriculum. To support this argument, we discuss how universities are uniquely positioned to address the potential benefits, downsides, and opportunities that are inherent in the multiple pathways available for becoming a cybersecurity professional. Additionally, we argue that simply covering security across all IS courses through modules or offering IT security as an elective course is an insufficient way to address security. We proposed a research methodology that will use an industry fit-gap approach to assess current and future cybersecurity needs and advocate for the inclusion of IT security as an core course in IS curriculum.

Keywords

Education, IS Curriculum, IT Security, Cybersecurity

Introduction

The information systems within organizations have become more complex, interdependent, and dispersed; they are merged with the information systems of partners, suppliers, and intermediaries (Ten et al. 2008). Four contributors to this phenomenon are the "internet of things (IOT)", "the cloud", "cyber-physical systems", and the increased digitization of organizational business processes and architectures. We use the term digital infrastructures to refer to one or a combination of the four deployed by an organization. As digital infrastructures become more prevalent, there will likely be a blurring of organizational and other information system boundaries. Information systems boundaries can appear at various levels (transactional, operational, or strategic) within an organization; where threats and opportunities can become apparent as data crosses each boundary (Farrell, 2008). The pace of technological change has made it difficult for any single organization to be able to protect its infrastructure independently because information security is a complex ecosystem of attackers and defenders involved in a perpetual game of cat and mouse (Knapp et al. 2003). This significantly increases cyber-risks to organizations who do not properly manage threats and opportunities from employees, intermediaries, contractors, partners, suppliers, governments, and even regulators.

A recent report by the New York Times indicates that by 2021 there will be a shortage of 3.1 million cybersecurity professionals worldwide (Perhach, 2018) with at least a half million roles being unfilled in the United States (Morgan, 2016). This is a concern because currently, negative consequences from threats and missed opportunities in managing cyber-risks can best be described as mere inconveniences and recoverable financial losses to the organizations and the people impacted by them. This is possibly because they are not perceived as being life-altering. Daneels & Salter (1999), noted that in order to be taken seriously "cyber" threats would have to lead to "death, bodily injury, extended power outages, plane crashes, water contamination or catastrophic economic losses". However, over the last two decades these cyber-risks have increasingly become life altering especially for such digital infrastructures such as power grids, air traffic control, and water systems (See Nicholson et al. 2012 for a literature review).

There is a great need for the management information systems domain to better address the shortage of cybersecurity professionals by ensuring that IT security is considered as a core course in every IS curriculum across all universities. We also discuss how universities are uniquely positioned to address the potential downsides that are inherent in the multiple pathways for becoming a cybersecurity professional. We argue that the currently IS programs are providing insufficient security training through modules which do not provide a sufficient amount of detail on IT security as required in the current technological environment and through separate elective IT security course.

The remainder of the paper is organized as follows. We discuss why the current paradigm for IT security[1] curriculums at 4 year universities are insufficient and the proposed knowledge areas that should be part of a core IT security course, this is followed by a discussion of the consequences and opportunities of the current various pathways for addressing the impending shortfall of cybersecurity professionals. This is followed by a proposed research design and lastly, we conclude with next steps for this research project.

Cybersecurity Needs in IS Curriculum

The Association of Computing Machinery (ACM) formed an inter-disciplinary task force where they highlighted the body of knowledge for cybersecurity (Burley et al. 2017). The task force composed of representatives from major computer science and information systems associations identified eight (8) security knowledge areas: data, software, component, connection, system, human, organization, and societal; and six (6) cross-cutting concepts: confidentiality, integrity, availability, risk, adversarial thinking, and systems thinking. Current IS courses do a great job incorporating the cross-cutting concepts into the cores IS courses. For example, most intro IS courses have a significant focus on integrity, risk, and systems thinking. However, in today's technologically focused environment, there is a significant need for IS students to have a strong foundation in the knowledge areas.

Data security refers to the protection of data, including storage, processing, and transmission. Software security refers to software development and usage in a way that does not compromise the security of the system it is used on or the information that it utilizes. Component Security refers to ensuring that all components integrated into a larger system are securely design, tested, and utilized. Connection security focuses on basic security knowledge of digital communications and networking. System security refers to understanding the importance of a holistic view of the security for a system, considering its components, connections, and software. Human security focuses on protecting individual employee data and understanding human behavior in a cybersecurity context. Organization security refers to the security policies, laws, regulations, standards, that a majority of organizations must adhere to. Lastly, societal security refers to the impacts of cybersecurity on society, specifically its positive or negative impacts.

It is important for IS students to have a strong foundation in these specific areas of security. Though some knowledge areas are more technical than others, such as component and system security, it is important for students to understand all the varied aspects of security in order to improve an organization's overall security. When the IT security course is only available as an elective amongst a large number of other choices, IS students may opt for analytics courses or other trending topics rather than the security course. A standalone IT Security course in the IS curriculum would allow IS professors to directly address each of the content areas as highlighted by the review of cybersecurity curriculum needs.

Consequences and Opportunities

There are many pathways for addressing the shortage of cybersecurity professionals including industry certifications/bootcamps, on the job training, community/technical colleges, universities, and advanced degree programs. It is unclear however the percentage or number of cybersecurity professionals that comprise each of the pathways. What makes IT security unique are that there are many pathways to an education including industry certifications which are significantly less than the cost of a four year degree and arguably may be more important than a traditional four year degree. Organizations with unfilled needs for cybersecurity personnel are taking a more hands on approach by providing on the job training

[1] In this study, IT security includes one or more of the following: internet security; privacy, data, information, or information system(s) related security. The terms IT security and cybersecurity are used interchangeably in this study.

to ensure they have the workforce that they need. However, there can be downsides to not obtaining a formal education. Table 1 outlines each of the pathways into a cybersecurity career and the benefits, downsides, and opportunities that universities can provide for each of these pathways to maximize the output of cybersecurity professionals in order to meet the impending demand for workers.

Pathways	Benefits	Downsides	Opportunities
Industry certifications and bootcamps	• Demonstrates competency • Peer recognition • Short pathway to employment	• Lack of formal education • Maybe missing foundational knowledge of the field • Restricted to practitioner role • Bootcamps are expensive	• Create formalized university certificate programs
On the job training	• Extensive hands on training • Pay while training • No student loan debt	• Limited upward mobility and pay increases • Company specific training • Limited lateral mobility to another company	• Work with companies to better understand skillset needs
2- Year College	• Focused and specific curriculum • Extensive hands on training • Status of a formal education	• Less social status • Similar downsides to industry certifications and on the job training	• Provide opportunities for development of soft skills and leadership training
4-Year College	• Social status • Broad general knowledge base including basic professional communication skills	• Student loan debt • Need to obtain certifications • Little-to-no hands on training • Possibility of outdated curriculum/little focus on security	• Offering IT security course as part of core curriculum within IS
Post-baccalaureate degree	• Amenability for leadership roles within companies • Training to research, create, and disseminate knowledge	• Student loan debt • Terminal degree • May lack hands on training • Possibility of outdated curriculum and need to seek even more education	• Offering IT security course as part of core curriculum within IS • Ensuring curriculum offers opportunity for hands on training

Table 1. Pathways to Cybersecurity Career

Proposed Research Design

Numerous business assessments have identified the lack of security focus in current graduates of undergraduate programs, both computer science (Morgan 2016) and information systems programs. Using extant research as a guide (Davis et al. 2003) Figure 1 provides an overview of the proposed research method for this study. The aim is to complete the following steps to identify the gap between industry needs and curriculum objectives: 1) identify the top security certifications and boot camps; 2) identify the top on the job training programs; 3) identify the top 2-year college, and 4-year universities, and4) graduate programs that offer IT security programs; and 5) identify current IT security job postings from a popular internet job board across occupations based on the 2019 DHS Directive[2]. We will then extract key terms phrases and categorize the key competencies and capabilities for those IT security positions. Lastly, we will provide exemplary IT security courses from IS programs that address the cybersecurity needs as identified above

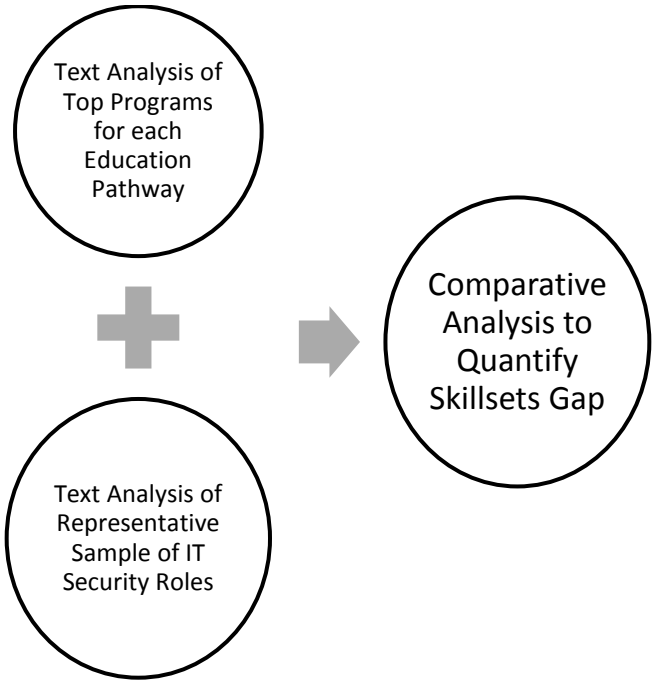

Figure 1: Research Methodology Overview

Currently, we are thoroughly reviewing the curriculum at the 10 best information systems programs, according to US News (US News 2018), to identify whether or not an IT security course was included in the core curriculum. Upon preliminary review, we found few programs that explicitly included a security course in the core curriculum. Though most programs probably include a module on security or incorporate security throughout the other core courses, this was not explicitly described on their public facing websites. Our proposed research methodology allows us to readily quantify the skillsets gaps between the various education pathways and current and emerging employment opportunities in the cybersecurity domain. The hope is that this research not only provides an opportunity to define the problem space but also opportunities for a solution. We will be able to visualize what specific education pathways are more relevant to addressing the skillsets gap, which education pathways need improvement,

[2] Criteria for selecting occupations which are considered to be IT security related will be selected based on the April 25th, 2019, directive from the Department of Homeland Security (DHS) that identified seven high-level categories of occupations each comprised of several specialty areas, which are considered "cybersecurity"; but no specific occupations, are listed in the directive (National Initiative for Cybersecurity Careers and Studies, 2017).

and which specific IT security occupations are more at risk of not having adequately training practitioners compared with others.

Conclusion

In this paper, we discussed the emerging issue of the shortage of cybersecurity professionals. As IT systems become more interconnected and dispersed the impacts from IT security failures have the potential to be catastrophic events which makes the need for qualified cybersecurity professionals even more urgent. This paper proposes a solution focusing on the 8 security areas identified in a report by the The Association of Computing Machinery (ACM) which formed a task force to highlight the body of knowledge for cybersecurity curriculums. In addition, this paper discusses additional pathways to addressing the shortfall of cybersecurity professionals and how universities are uniquely positioned to address the downsides that other pathways may present.

REFERENCES

Burley,D.,Bishop,M,.Buck,S.,Ekstrom,J,.Futcher,L.,Gibson,D.,Hawthorne,E.,Kaza,S.,Levy,Y., Mattord, H., Parrish, A. 2017. "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity." Joint Task Force on Cybersecurity Education, December 31 2017, (https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, accessed May 1, 2019).

Daneels, A., and Salter, W. 1999. "What Is SCADA", Proceedings of the 7th International Conference on Accelerator and Large Experimental Physics Control Systems, NA(eds.), Trieste, Italy, pp.339-343.

Davis, S., Siau, K., and Dhenuvakonda, K. 2003. "A Fit-Gap Analysis of e-Business Curricula vs. Industry Needs," Communications of the ACM (46:12), pp. 167–177.

Farrell, S. 2008. Security Boundaries. IEEE Internet Computing, (12:1), pp. 93-96.

Knapp, K., Morris, F., Rainer Jr, R. K., and Byrd, T. A. 2003. "Defense Mechanisms of Biological Cells: A Framework for Network Security Thinking," Communications of the Association for Information Systems (12:1), pp. 701-719.

Morgan, S. 2016. "Top U.S. Computer Science Undergrad Programs Flunk Cybersecurity," Forbes, April 14. (https://www.forbes.com/sites/stevemorgan/2016/04/14/top-u-s-computer-science-undergrad-programs-flunk-cybersecurity/, accessed February 27, 2019).

National Initiative for Cybersecurity Careers and Studies. 2019. "Cybersecurity Workforce Framework," Department of Homeland Security, (https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework, accessed May 1, 2019).

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). "SCADA Security in Light of Cyber-Warfare." Computers and Security, (31:4), pp.418-436.

Perhach, P. 2018. 'The Mad Dash to Find a Cybersecurity Workforce." The New York Time,November 7th 2018,(https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html, accessed May 1, 2019).

Ten, C.-W., Liu, C.-C., and Manimaran, G. 2008. "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems (23:4), pp. 1836–1846.

US News. 2018. "The Best Information Systems Programs, Ranked," December. (https://www.usnews.com/best-graduate-schools/top-business-schools/information-systems-rankings, accessed February 28, 2019).